Remarks

In the office action, the Examiner rejected claims 1 - 12 and 21 - 29 under 35 USC § 102(e) as being anticipated by US Patent 5,960,080 (issued Sep. 28, 1999; hereinafter "Fahlman"). The Examiner also rejected claims 13 - 20 under 35 USC § 103(a) as being unpatentable over Fahlman in view of US Patent 4,882,752 (issued Nov. 21, 1989; hereinafter Lindman). The Applicant respectfully traverses the rejections and submits the following arguments.

Claims 1 - 12

In claim 1, the Applicant recites a method for use in a multi-level secure system for sanitizing a message. The multilevel secure system includes at least first and second security levels with the first security level users being authorized to receive sensitive information that second security level users are not authorized to receive. The Applicant has amended this method merely to improve clarity of the claim.

The method includes steps of establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules and using the computer-based sanitization tool to receive a first message from a first external system. The first message includes the sensitive information as well as additional information. The sensitive information is associated with the first security level. The method also includes a step of operating the computer-based sanitization tool to identify the sensitive information within the message and to sanitize the message relative to the sensitive information, thereby generating a first sanitized message that differs from the first message. Additionally, the method includes a step of operating the computer-based sanitization tool for transmission of the first sanitized message to a second external system that is associated with the second security level.

Fahlman teaches identifying terms of a message that a message sender deems as sensitive, such as names and other personal information. The message sender then temporarily replaces the sensitive terms with tokens to generate a new message containing the tokens. *See e.g.*, column 45, lines 38 – 46. The new token containing message may then be sent to another person for additional processing (e.g., translation). Once the processing is finished, the subsequent processor reconveys the processed message, still containing the tokens, back to the message

sender such that the tokens may be replaced with their corresponding original sensitive terms. Such a process differs from the Applicant's claim because, among other reasons, Fahlman does not receive a message from a first system and transmit it to a second system after sanitization. Rather, Fahlman teaches transmitting a sanitized message back to the first system.

If and when the message that Fahlman teaches is transmitted to a second system, the message is not sanitized. A message in Fahlman is temporarily conveyed to another for intermediate processing. Upon such intermediate processing, the message is reconveyed to the message originator for merging the original sensitive terms with the message. In other words, temporary tokens are replaced with the original sensitive terms. *See e.g.*, column 5, lines 14 - 37. Contrarily, a message of the Applicant's claims is sanitized and transmitted to an external system associated with a lesser security level (i.e., first security level users are authorized to receive sensitive information that second security level users are not authorized to receive). The Applicant's claims are therefore paramount to dissemination of information where sensitive information is continually protected.

To further clarify the difference between the intermediate processing of information of Fahlman and the dissemination of information of the Applicant's claims, the Applicant has amended claim 1 to recite that the sensitive information is associated with the first security level. With the message sanitized of sensitive information and a first sanitized message generated therefrom, the first sanitized message may be transmitted to a second external system that is associated with a second security level (i.e., a lesser security level because the second security level is not authorized to see the sensitive information). The Applicant believes this amendment illustrates the distinguishing features of the Applicant's claim.

The Applicant maintains that claim 1 is novel in view of Fahlman. The Applicant therefore respectively requests reconsideration and allowance of claim 1. Claims 2 - 12 depend from independent claim 1 and inherit all of the novel features of the independent claim. However, these claims require subject matter that further distinguishes the claims from Fahlman. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claims 2 - 12.

Claims 13 - 20

In claim 13, the Applicant recites a method for use in a multi-level secure system for sanitizing a message. The method includes steps of establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules, using the computer-based sanitization tool to receive a message for potential distribution, and operating the computer-based sanitization tool to identify at least first and second potential recipients having first and second security clearances, respectively. For example, some users may be associated with a first security level whereas others are associated with a second security level that do not have access to certain information that the first security level users have.

The method further includes a step of operating the computer-based sanitization tool to sanitize a received message and generate a first sanitized message for transmission to the first potential recipient. The method also includes a step of operating the computer-based sanitization tool for sanitizing the received message to generate a second sanitized message for transmission to the second potential recipient. This second message differs from the first sanitized message in that the first sanitized message contains information that the second potential recipient is not allowed to receive.

Although the arguments of claim 1 may apply herein as well, the Examiner states that Fahlman teaches all of the elements of the Applicant's claim 13 except for operating a computer-based tool for identifying first and second potential recipients having first and second security clearances, respectively. The Applicant agrees with this assertion and adds that Fahlman, in fact, does not teach using the computer-based tool to identify anyone. Rather, a sender associated with the message identifies a recipient of a sanitized message for transmission thereto. *See e.g.*, column 4, lines 47 - 59. Regardless, Fahlman also does not teach operating a computer-based sanitization tool for sanitizing a received message to generate first and second sanitized messages that differ based on respective first and second security levels.

While Fahlman does not teach generating multiple messages respectively based on multiple security levels, Lindman certainly adds nothing to Fahlman to teach such features. The Examiner states that Lindman teaches identifying first and second sensitive information based on first and second security clearances without specifically mentioning where Lindman allegedly teaches operating a computer-based sanitization tool for identifying first and second potential

recipients having first and second security clearances, respectively. Regardless, the Applicant submits that such an assertion is incorrect and that Lindman does not even teach identifying first and second sensitive information. Rather, Lindman teaches computer systems having different security levels that access a main computer through a master security control processor ("SCP"). The SCP acts as a sort of gatekeeper to the main computer to prevent other computers from unauthorized access (*see e.g.*, column 8, lines 24 - 30 of Lindman). This control is based on identification of an accessing computer's security level. Nowhere, however, does Lindman teach identifying sensitive information.

To establish a *prima facie* case obviousness, the Examiner must show that all of the claim limitations of the Applicant's claims are taught. Additionally, there must be some reasonable suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Finally, there must be a reasonable expectation of success in the combination. The Applicant maintains that Fahlman is deficient not only with respect to what the Examiner states but also because Fahlman does not teach generating first and second sanitized messages. It is clear from Lindman that Lindman adds nothing to Fahlman to supplement Fahlman as the Examiner suggests. But it is also true that Lindman adds nothing to supplement Fahlman with respect to generating to sanitized messages. Regardless, Lindman provides no teaching or reasonable suggestion to combine with Fahlman.

The Applicant maintains that the Lindman reference provides no teaching or reasonable suggestion to combine with Fahlman, a reference which is almost 10 years younger. Aside from that, however, the Applicant maintains that Fahlman also does not provide a teaching or reasonable suggestion to combine with Lindman, particularly because the two references are directed towards different fields. For example, Fahlman is directed to message transformation whereas Lindman is directed to computer security. Because there is no teaching or reasonable suggestion to combine the references and because the references do not teach all of the Applicant's claim elements, Fahlman and Lindman are simply insufficient as prior art references.

The Applicant maintains claim 13 is novel and nonobvious in view of Fahlman and Lindman, either alone or in combination. The Applicant therefore respectfully requests reconsideration and allowance of claim 13. Claims 14 - 20 depend from claim 13 and inherit all

of the novel and nonobvious features of the independent claim. However, these claims require additional features that further distinguish from the cited references. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claims 14 - 20.

Claims 21 - 20

In claim 21, the Applicant recites a method for use in a multilevel secure system for sanitizing a message. The multilevel secure system includes first and second security levels such that first security level users are authorized to receive sensitive information that second security level users are not authorized to receive. The method includes establishing a computer-based sanitization tool for sanitizing messages based on predefined sanitization rules. The method also includes operating the computer-based sanitization tool for receiving a message and recursively parsing the message such that the message is parsed into tokens of a desired size. The method also includes operating the computer-based sanitization tool for applying sanitization rules with respect to the parsed tokens to identify at least one dirty token relative to an unidentified recipient. Furthermore, the method includes operating the tool for sanitizing the message relative to the dirty token to generate a sanitized message for transmission to the indemnified recipient.

Again, Fahlman teaches identifying terms of a message that a message sender deems as sensitive. However, such identification is not based on a recipient. Rather, the sender determines the sensitivity of the information (see e.g., column 4, lines 29 - 31 of Fahlman). Although Fahlman's identification of sensitive information is not based on a recipient, Fahlman also teaches a method of temporarily replacing sensitive terms with tokens for subsequent processing of a message that differs from the Applicant's claims.

In Fahlman, a message sender temporarily replaces sensitive terms with tokens to generate a new message containing the tokens. The new token containing message may then be sent to another person for additional processing (e.g., translation). Once the processing is finished, the subsequent processor reconveys the processed message, still containing the tokens, back to the message sender such that the tokens may be replaced with their corresponding original sensitive terms. Such a process differs from the Applicant's claim because, among other reasons, the Applicant does not claim temporary replacement of the sensitive terms with tokens..

As discussed hereinabove, one difference between the temporary replacement of Fahlman

and the Applicant's claims regards the dissemination of messages. For example, Fahlman does not receive a message from a first system and transmit it to a second system after sanitization. Rather, Fahlman teaches transmitting a sanitized message back to the first system.

If and when the message that Fahlman teaches is transmitted to a second system, the message is not sanitized. A message in Fahlman is temporarily conveyed to another for intermediate processing. Upon such intermediate processing, the message is reconveyed to the message originator for merging the original sensitive terms with the message. In other words, temporary tokens are replaced with the original sensitive terms. *See e.g.*, column 5, lines 14 - 37. Contrarily, a message of the Applicant's claims is sanitized and transmitted to an external system associated with a lesser security level (i.e., first security level users are authorized to receive sensitive information that second security level users are not authorized to receive). Again, the Applicant's claims are therefore paramount to dissemination of information where sensitive information is continually protected.

The Applicant maintains that claim 21 is novel in view of Fahlman. The Applicant therefore respectively requests reconsideration and allowance of claim 21. Claims 22 - 26 depend from independent claim 21 and inherit all of the novel features of the independent claim. However, these claims require subject matter that further distinguishes the claims from Fahlman. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claims 22 - 26.

Claims 27 - 29

In claim 27, the Applicant recites an apparatus for use in a multilevel secure system for sanitizing a message. The multilevel secure system includes first and second security levels such that a first security level user is authorized to receive sensitive information that a security level user is not authorized to receive. The apparatus includes an interface engine including a generic processing module for performing a transformation process relative to an information stream associated with an external system. The generic processing module is adaptable to handle messages and multiple forms associated with multiple external systems. The apparatus also includes a storage structure for storing first external specification information relating to a first external form of a first external system and second external specification information relating to

a second external form of a second external system.

The interface engine is operative to identify an external form associated with a message. The interface engine also accesses the storage to obtain a corresponding specification. The apparatus also includes a second storage structure for storing sanitization rules and a sanitization engine operative for accessing the second storage structure to obtain at least one sanitization rule. The sanitization engine is also operative for sanitizing the message based on the sanitization rule.

In Fahlman, a message sender temporarily replaces sensitive terms with tokens to generate a new message containing the tokens. The new token containing message may then be sent to another person for additional processing (e.g., translation). Once the processing is finished, the subsequent processor reconveys the processed message, still containing the tokens, back to the message sender such that the tokens may be replaced with their corresponding original sensitive terms. Such a process differs from the Applicant's claim because, among other reasons, the Applicant does not receive a message from a first system and transmit it to a second system after sanitization. Rather, Fahlman teaches transmitting a sanitized message back to the first system.

If and when the message that Fahlman teaches is transmitted to a second system, the message is not sanitized. A message in Fahlman is temporarily conveyed to another for intermediate processing. Upon such intermediate processing, the message is reconveyed to the message originator for merging the original sensitive terms with the message. In other words, temporary tokens are replaced with the original sensitive terms. *See e.g.*, column 5, lines 14 - 37. The Applicant however claims an interface engine for performing a transformation process relative to an information stream associated with an external system. The Applicant also claims a sanitization engine operative for accessing a storage structure to obtain a sanitization rule for sanitizing a message based on the sanitization rule. The Applicant maintains that such a sanitization engine differs from Fahlman because, among other reasons, the sanitization engine relates to dissemination of information where sensitive information is continually protected as described hereinabove.

The Applicant maintains that claim 27 is novel in view of Fahlman. The Applicant therefore respectively requests reconsideration and allowance of claim 27. Claims 28 - 29 depend from independent claim 27 and inherit all of the novel features of the independent claim.

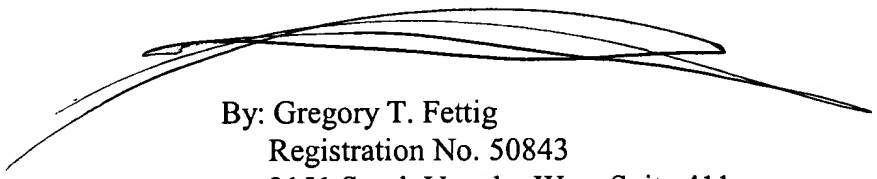
However, these claims require subject matter that further distinguishes the claims from Fahlman. For at least these reasons, the Applicant respectfully requests reconsideration and allowance of claims 28 - 29.

Conclusion

Based upon the foregoing, the Applicant believes that all pending claims are in condition for allowance and such disposition is respectfully requested. In the event that a telephone conversation would further prosecution and/or expedite allowance, the Examiner is invited to contact the undersigned.

Respectfully submitted,

MARSH FISCHMANN & BREYFOGLE LLP



By: Gregory T. Fettig
Registration No. 50843
3151 South Vaughn Way, Suite 411
Aurora, Colorado 80014
(303) 338-0997

Date: Jun. 27, 2005